

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF TEXAS  
WACO DIVISION

SABLE NETWORKS, INC. AND  
SABLE IP, LLC,

*Plaintiffs,*

v.

SONICWALL INC.,

*Defendant.*

Civil Action No. \_\_\_\_\_

**JURY TRIAL DEMANDED**

**COMPLAINT FOR PATENT INFRINGEMENT**

Sable Networks, Inc. and Sable IP, LLC (collectively, “Sable” or “Plaintiffs”) bring this action and make the following allegations of patent infringement relating to U.S. Patent Nos.: 6,954,431 (the “431 patent”); 6,977,932 (the “932 patent”); 7,630,358 (the “358 patent”); and 8,243,593 (the “593 patent”) (collectively, the “patents-in-suit”). Defendant SonicWall Inc. (“SonicWall” or “Defendant”) infringes the patents-in-suit in violation of the patent laws of the United States of America, 35 U.S.C. § 1 *et seq.*

**INTRODUCTION**

1. The patents-in-suit arise from technologies developed by Dr. Lawrence G. Roberts - one of the founding fathers of the internet.<sup>1</sup> The patents relate to technologies for efficiently managing the flow of data packets over routers and switch devices. Dr. Roberts and engineers at Caspian Networks, Inc. and later Sable Networks, Inc. developed these technologies to address the increasing amount of data sent over computer networks.

---

<sup>1</sup> Chris Woodford, THE INTERNET: A HISTORICAL ENCYCLOPEDIA VOLUME 2 at 204 (2005) (“Widely regarded as one of the founding fathers of the Internet, Lawrence Roberts was the primary architect of ARPANET, the predecessor of the Internet.”).

2. Dr. Roberts is best known for his work as the Chief Scientist of the Advanced Research Projects Agency (ARPA) where he designed and oversaw the implementation of ARPANET, the precursor to the internet. Dr. Roberts' work on ARPANET played a key role in the development of digital network transmission technologies.<sup>2</sup> Initially, ARPANET was used primarily to send electronic mail and Dr. Roberts developed the first program for reading and sending electronic messages.



Keenan Mayo and Peter Newcomb, *How The Web Was Won*, VANITY FAIR at 96-97 (January 7, 2009); *One of the Engineers Who Invented the Internet Wants to Build A Radical new Router*, IEEE SPECTRUM MAGAZINE (July 2009); Katie Hafner, *Billions Served Daily, and Counting*, N.Y. TIMES at G1 (December 6, 2001) (“Lawrence Roberts, who was then a manager at the Advanced Research Projects Agency’s Information Processing Techniques Office, solved that problem after his boss began complaining about the volume of e-mail piling up in his in box. In 1972, Dr. Roberts produced the first e-mail manager, called RD, which included a filing system, as well as a Delete function.”).

3. Dr. Roberts' work on ARPANET played a key role in the development of packet switching networks. Packet switching is a digital network transmission process in which data is broken into parts which are sent independently and reassembled at a destination. Electronic messages sent over the ARPANET were broken up into packets then routed over a network to a destination. “In designing the ARPANET, Roberts expanded on the work he'd done at MIT, using

---

<sup>2</sup> Katie Hafner, *Lawrence Roberts, Who Helped Design Internet’s Precursor*, N.Y. TIMES at A2 (December 31, 2018) (“Dr. Roberts was considered the decisive force behind packet switching, the technology that breaks data into discrete bundles that are then sent along various paths around a network and reassembled at their destination.”).

those tiny data packets to send information from place to place.”<sup>3</sup> Packet switching has become the primary technology for data communications over computer networks.



George Johnson, *From Two Small Nodes, a Mighty Web Has Grown*, N.Y. TIMES at F1 (October 12, 1999).

4. After leaving ARPANET, Dr. Roberts grew increasingly concerned that existing technologies for routing data packets were incapable of addressing the increasing amounts of data traversing the internet.<sup>4</sup> Dr. Roberts identified that as the “Net grows, the more loss and transmission of data occurs. Eventually, gridlock will set in.”<sup>5</sup>

***The Internet is broken. I should know: I designed it.*** In 1967, I wrote the first plan for the ancestor of today's Internet, the Advanced Research Projects Agency Network, or ARPANET, and then led the team that designed and built it. The main idea was to share the available network infrastructure by sending data as small, independent packets, which, though they might arrive at different times, would still generally make it to their destinations. The small computers that directed the data traffic—I called them Interface Message Processors, or IMPs—evolved into today's routers, and for a long time they've kept up with the Net's phenomenal growth. Until now.

Lawrence Roberts, *A Radical New Router*, IEEE SPECTRUM Vol. 46(7) at 34 (August 2009) (emphasis added).

<sup>3</sup> Code Metz, *Larry Roberts Calls Himself the Founder of The Internet. Who Are You To Argue*, WIRED MAGAZINE (September 24, 2012); John C. McDonald, FUNDAMENTALS OF DIGITAL SWITCHING at 211 (1990) (“The ARPANET was, in part, an experimental verification of the packet switching concept. Robert's objective was a new capability for resource sharing.”).

<sup>4</sup> eWeek Editors, *Feeling A Little Congested*, E WEEK MAGAZINE (September 24, 2001) (“Lawrence Roberts, one of the primary developers of Internet precursor ARPANet and CTO of Caspian Networks, recently released research indicating that Net traffic has quadrupled during the past year alone.”).

<sup>5</sup> Michael Cooney, *Can ATM Save The Internet*, NETWORK WORLD at 16 (May 20, 1996); Lawrence Roberts, *A RADICAL NEW ROUTER*, IEEE Spectrum Vol. 46 34-39 (August 2009).

5. In 1998, Dr. Roberts founded Caspian Networks.<sup>6</sup> At Caspian Networks, Dr. Roberts developed a new kind of internet router to efficiently route packets over a network. This new router was aimed at addressing concerns about network “gridlock.” In a 2001 interview with Wired Magazine, Dr. Roberts discussed the router he was developing at Caspian Networks – the Apeiro. “Roberts says the Apeiro will also create new revenue streams for the carriers by solving the ‘voice and video problem.’ IP voice and video, unlike email and static Web pages, breaks down dramatically if there's a delay - as little as a few milliseconds - in getting packets from host to recipient.”<sup>7</sup>



Jim Duffy, *Router Newcomers take on Cisco, Juniper*, NETWORK WORLD at 14 (April 14, 2013); Stephen Lawson, *Caspian Testing Stellar Core Offering*, NETWORK WORLD at 33 (December 17, 2001); Tim Greene, *Caspian Plans Superfast Routing For The 'Net Core*, NETWORK WORLD at 10 (January 29, 2001); Andrew P. Madden, *Company Spotlight: Caspian Networks*, MIT TECHNOLOGY REVIEW at 33 (August 2005); and Loring Wirbel, *Caspian Moves Apeiro Router To Full Availability*, EE TIMES (April 14, 2003).

6. The Apeiro debuted in 2003. The Apeiro, a flow-based router, can identify the nature of a packet – be it audio, text, or video, and prioritize it accordingly. The Apeiro included

<sup>6</sup> Caspian Networks, Inc. was founded in 1998 as Packetcom, LLC and changed its name to Caspian Networks, Inc. in 1999.

<sup>7</sup> John McHugh, *The n-Dimensional Superswitch*, WIRED MAGAZINE (May 1, 2001).

numerous technological advances including quality of service (QoS) routing and flow-based routing.

7. At its height, Caspian Networks Inc. raised more than \$300 million dollars and grew to more than 320 employees in the pursuit of developing and commercializing Dr. Roberts' groundbreaking networking technologies, including building flow-based routers that advanced quality of service and load balancing performance. However, despite early success with its technology and business, Caspian hit hard times when the telecommunications bubble burst.

8. Sable Networks, Inc. was formed by Dr. Sang Hwa Lee to further develop and commercialize the flow-based networking technologies developed by Dr. Roberts and Caspian Networks.<sup>8</sup> Sable Networks, Inc. has continued its product development efforts and has gained commercial success with customers in Japan, South Korea, and China. Customers of Sable Networks, Inc. have included: SK Telecom, NTT Bizlink, Hanaro Telecom, Dacom Corporation, USEN Corporation, Korea Telecom, China Unicom, China Telecom, and China Tietong.

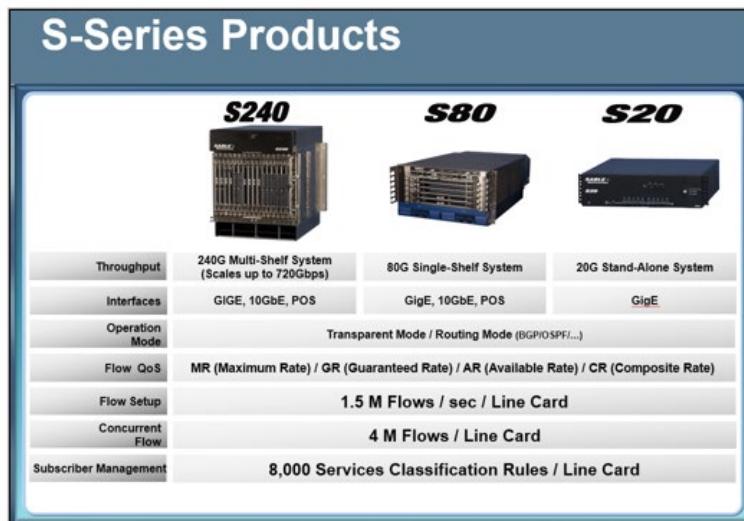


*SK Telecom and Sable Networks Sign Convergence Network Deal*, COMMS UPDATE – TELECOM NEWS SERVICE (February 4, 2009) (“South Korean operator SK Telecom has announced that it has signed a deal with US-based network and solutions provider Sable Networks.”); *China Telecom Deploys Sable*, LIGHT READING NEWS FEED (November 19, 2007) (“Sable Networks Inc., a leading

<sup>8</sup> Dr. Lee, through his company Mobile Convergence, Ltd. purchased the assets of Caspian Networks Inc. and subsequently created Sable Networks, Inc.

provider of service controllers, today announced that China Telecom Ltd, the largest landline telecom company in China, has deployed the Sable Networks Service Controller in their network.”).

9. Armed with the assets of Caspian Networks Inc. as well as members of Caspian Networks’ technical team, Sable Networks, Inc. continued the product development efforts stemming from Dr. Roberts’ flow-based router technologies. Sable Networks, Inc. developed custom application-specific integrated circuits (“ASIC”) designed for flow traffic management. Sable Network, Inc.’s ASICs include the Sable Networks SPI, which enables 20 Gigabit flow processing. In addition, Sable Networks, Inc. developed and released S-Series Service Controllers (e.g., S80 and S240 Service Controller models) that contain Sable Networks’ flow-based programmable ASICs, POS and Ethernet interfaces, and carrier-hardened routing and scalability from 10 to 800 Gigabits.



SABLE NETWORKS S-SERIES SERVICE CONTROLLERS (showing the S240-240G Multi-Shelf System, S80-80G Single-Shelf System, and S20-20G Stand-Alone System).

10. Sable pursues the reasonable royalties owed for SonicWall’s use of the inventions claimed in Sable’s patent portfolio, which arise from Caspian Networks and Sable Networks’ groundbreaking technology.

### **SABLE'S PATENT PORTFOLIO**

11. Sable's patent portfolio includes over 34 patent assets, including 14 granted U.S. patents. Dr. Lawrence Roberts' pioneering work on QoS traffic prioritization, flow-based switching and routing, and the work of Dr. Roberts' colleagues at Caspian Networks Inc. and Sable Networks, Inc. are claimed in the various patents owned by Sable.

12. Highlighting the importance of the patents-in-suit is the fact that the Sable's patent portfolio has been cited by over 1,000 U.S. and international patents and patent applications assigned to a wide variety of the largest companies operating in the computer networking field. Sable's patents have been cited by companies such as:

- Cisco Systems, Inc.<sup>9</sup>
- Juniper Networks, Inc.<sup>10</sup>
- Broadcom Limited<sup>11</sup>
- EMC Corporation<sup>12</sup>
- F5 Networks, Inc.<sup>13</sup>
- Verizon Communications Inc.<sup>14</sup>
- Microsoft Corporation<sup>15</sup>
- Intel Corporation<sup>16</sup>
- Extreme Networks, Inc.<sup>17</sup>
- Huawei Technologies Co., Ltd.<sup>18</sup>

---

<sup>9</sup> See, e.g., U.S. Patent Nos. 7,411,965; 7,436,830; 7,539,499; 7,580,351; 7,702,765; 7,817546; 7,936,695; 8,077,721; 8,493,867; 8,868,775; and 9,013,985.

<sup>10</sup> See, e.g., U.S. Patent Nos. 7,463,639; 7,702,810; 7,826,375; 8,593,970; 8,717,889; 8,811,163; 8,811,183; 8,964,556; 9,032,089; 9,065,773; and 9,832,099.

<sup>11</sup> See, e.g., U.S. Patent No. 7,187,687; 7,206,283; 7,266,117; 7,596,139; 7,649,885; 8,014,315; 8,037,399; 8,170,044; 8,194,666; 8,271,859; 8,448,162; 8,493,988; 8,514,716; and 7,657,703.

<sup>12</sup> See, e.g., U.S. Patent Nos. 6,976,134; 7,185,062; 7,404,000; 7,421,509; 7,864,758; and 8,085,794.

<sup>13</sup> See, e.g., U.S. Patent Nos. 7,206,282; 7,580,353; 8,418,233; 8,565,088; 9,225,479; 9,106,606; 9,130,846; 9,210,177; 9,614,772; 9,967,331; and 9,832,069.

<sup>14</sup> See, e.g., U.S. Patent Nos. 7,349,393; 7,821,929; 8,218,569; 8,289,973; 9,282,113; and 8,913,623.

<sup>15</sup> See, e.g., U.S. Patent Nos. 7,567,504; 7,590,736; 7,669,235; 7,778,422; 7,941,309; 7,636,917; 9,571,550; and 9,800,592.

<sup>16</sup> See, e.g., U.S. Patent Nos. 7,177,956; 7,283,464; 9,485,178; 9,047,417; 8,718,096; 8,036,246; 8,493,852; and 8,730,984.

<sup>17</sup> See, e.g., U.S. Patent Nos. 7,903,654; 7,978,614; 8,149839; 10,212,224; 9,112,780; and 8,395,996.

<sup>18</sup> See, e.g., U.S. Patent Nos. 7,903,553; 7,957,421; 10,015,079; 10,505,840; and Chinese Patent

**THE PARTIES**

**SABLE NETWORKS, INC.**

13. Sable Networks, Inc. (“Sable Networks”) is a corporation organized and existing under the laws of the State of California.

14. Sable Networks was formed to continue the research, development, and commercialization work of Caspian Networks Inc., which was founded by Dr. Lawrence Roberts to provide flow-based switching and routing technologies to improve the efficiency and quality of computer networks.

15. Sable Networks is the owner by assignment of all of the patents-in-suit.

**SABLE IP, LLC**

16. Sable IP, LLC (“Sable IP”) is a Delaware limited liability company with its principal place of business at 225 S. 6th Street, Suite 3900, Minneapolis, Minnesota 55402. Pursuant to an exclusive license agreement with Sable Networks, Sable IP is the exclusive licensee of the patents-in-suit.

**SONICWALL INC.**

17. SonicWall Inc. (“SonicWall”), is a Delaware corporation with its principal place of business at 1033 McCarthy Blvd., Milpitas, CA 95035. SonicWall may be served through its registered agent Corporation Service Company, 251 Little Falls Drive, Wilmington, Delaware 19808.

18. SonicWall conducts business operations within the Western District of Texas where it sells, develops, and/or markets its products including facilities in Austin, Texas. Several key SonicWall employees work out of SonicWall’s Austin, Texas offices, including but not limited to

---

Nos. CN108028828 and CN106161333.

a Vice President of Web and Digital Experience, a Director of Marketing, and a Director of Finance.

**JURISDICTION AND VENUE**

19. This action arises under the patent laws of the United States, Title 35 of the United States Code. Accordingly, this Court has exclusive subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338(a).

20. This Court has personal jurisdiction over SonicWall in this action because SonicWall has committed acts within the Western District of Texas giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over SonicWall would not offend traditional notions of fair play and substantial justice. Defendant SonicWall, directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), has committed and continues to commit acts of infringement in this District by, among other things, offering to sell and selling products and/or services that infringe the patents-in-suit. SonicWall has offices and key employees located in Austin, Texas, and actively directs its activities to customers located in the State of Texas.

21. Venue is proper in this district under 28 U.S.C. §§ 1391(b)-(d) and 1400(b). Defendant SonicWall maintains a regular and established place of business in the Western District of Texas, has transacted business in the Western District of Texas, and has committed acts of direct and indirect infringement in the Western District of Texas.

22. SonicWall recently sought out the Western District of Texas as its preferred venue to defend itself against allegations of patent infringement. On July 2, 2020, SonicWall filed the following declaratory judgment action against Proven Networks, LLC in this District: *SonicWall Inc. v. Proven Networks, LLC*, C.A. No. 1:20-cv-00715 (W.D. Tex. July 2, 2020).

23. This Court has personal jurisdiction over SonicWall. SonicWall has conducted and does conduct business within the State of Texas. SonicWall, directly or through subsidiaries or intermediaries (including distributors, retailers, and others), ships, distributes, makes, uses, offers for sale, sells, imports, and/or advertises (including by providing an interactive web page) its products and/or services in the United States and the Western District of Texas and/or contributes to and actively induces its customers to ship, distribute, make, use, offer for sale, sell, import, and/or advertise (including the provision of an interactive web page) infringing products and/or services in the United States and the Western District of Texas. SonicWall, directly and through subsidiaries or intermediaries (including distributors, retailers, and others), has purposefully and voluntarily placed one or more of its infringing products and/or services, as described below, into the stream of commerce with the expectation that those products will be purchased and used by customers and/or consumers in the Western District of Texas. These infringing products and/or services have been and continue to be made, used, sold, offered for sale, purchased, and/or imported by customers and/or consumers in the Western District of Texas. SonicWall has committed acts of patent infringement within the Western District of Texas. SonicWall interacts with customers in Texas, including through visits to customer sites in Texas. Through these interactions and visits, SonicWall directly infringes the patents-in-suit. SonicWall also interacts with customers who sell the Accused Products into Texas, knowing that these customers will sell the Accused Products into Texas, either directly or through intermediaries.

24. SonicWall has minimum contacts with this District such that the maintenance of this action within this District would not offend traditional notions of fair play and substantial justice. Thus, the Court therefore has both general and specific personal jurisdiction over SonicWall.

### **THE ASSERTED PATENTS**

#### **U.S. PATENT No. 6,954,431**

25. U.S. Patent No. 6,954,431 (the “‘431 patent”) entitled, *Micro-Flow Management*, was filed on December 6, 2001, and claims priority to April 19, 2000. The ‘431 patent is subject to a 35 U.S.C. § 154(b) term extension of 722 days. Sable Networks, Inc. is the owner by assignment of the ‘431 patent. Sable IP is the exclusive licensee of the ‘431 patent. A true and correct copy of the ‘431 patent is attached hereto as Exhibit A.

26. The ‘431 patent discloses novel methods and systems for managing data traffic comprising a plurality of micro-flows through a network.

27. The inventions disclosed in the ‘431 patent improve the quality of service in data transmissions over a computer network by relying on per micro-flow state information that enables rate and delay variation requirements to be within set quantified levels of service.

28. The ‘431 patent discloses technologies that speed the rate at which data can effectively travel over a computer network by optimizing packet discarding.

29. The ‘431 patent discloses the use of micro-flow state information to determine the rate of each flow, thus optimizing discards and optimizing the quality of service of data transmission.

30. The ‘431 patent discloses methods and systems that avoid networking system degradation by not overloading network switch buffers.

31. The ‘431 patent discloses a method for managing data traffic through a network that determines a capacity of a buffer containing a micro-flow based on a characteristic.

32. The ‘431 patent discloses a method for managing data traffic through a network that assigns an acceptable threshold value for the capacity of the buffer over a predetermined period of time.

33. The ‘431 patent discloses a method for managing data traffic through a network that delegates a portion of available bandwidth in the network to the micro-flow.

34. The ‘431 patent discloses a method for managing data traffic through a network that uses the buffer for damping jitter associated with the micro-flow.

35. The ‘431 patent has been cited by 103 patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘431 patent as relevant prior art:

- Cisco Systems, Inc.
- Juniper Networks, Inc.
- Broadcom Limited
- Intel Corporation
- Sun Microsystems, Inc.
- Oracle Corporation
- Samsung Electronics Co., Ltd.
- Adtran, Inc.
- Time Warner Cable, Inc.
- FSA Technologies, Inc.
- Internap Corporation
- France Telecom
- The Boeing Company
- Wistar Trading, Ltd.

**U.S. PATENT No. 6,977,932**

36. U.S. Patent No. 6,977,932 (the “‘932 patent”) entitled, *System and Method for Network Tunneling Utilizing Micro-Flow State Information*, was filed on January 16, 2002. The ‘932 patent is subject to a 35 U.S.C. § 154(b) term extension of 815 days. Sable Networks, Inc. is the owner by assignment of the ‘932 patent. Sable IP is the exclusive licensee of the ‘932 patent. A true and correct copy of the ‘932 patent is attached hereto as Exhibit B.

37. The ‘932 patent discloses novel methods and apparatuses for utilizing a router capable of network tunneling utilizing flow state information.

38. The inventions disclosed in the '932 patent enable the use of micro-flow state information to improve network tunneling techniques.

39. The inventions disclosed in the '932 patent maintain flow state information for various quality of service characteristics by utilizing aggregate flow blocks.

40. The aggregate flow blocks disclosed in the '932 patent maintain micro-flow block information.

41. The technologies claimed in the '932 patent speed the flow of network traffic over computer networks by avoiding time consuming and processor intensive tasks by combining flow state information with other information such as label switched paths utilization information. This permits the micro-flows associated with an aggregate flow block to all be processed in a similar manner.

42. The technologies disclosed in the '932 patent result in more efficient computer networks by avoiding the processor intensive tasks of searching millions of flow blocks to identify flow blocks having certain micro-flow characteristics in order to process large numbers of micro-flows.

43. The '932 patent discloses a router capable of network tunneling utilizing flow state information containing an aggregate flow block having tunnel specific information for a particular network tunnel.

44. The '932 patent discloses a router capable of network tunneling utilizing flow state information containing a flow block having flow state information for a micro-flow, the flow block further including an identifier that associates the flow block with the aggregate flow block.

45. The '932 patent discloses a router capable of network tunneling utilizing flow state information wherein the aggregate flow block stores statistics for the particular network tunnel.

46. The ‘932 patent has been cited by 86 patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘932 patent as relevant prior art:

- Cisco Systems, Inc.
- Juniper Networks, Inc.
- Avaya, Inc.
- Fujitsu, Ltd.
- Intel Corporation
- Nokia Corporation
- Qualcomm, Inc.
- Sprint Communications Co.
- Telefonaktiebolaget LM Ericsson
- Verizon Communications, Inc.

**U.S. PATENT No. 7,630,358**

47. U.S. Patent No. 7,630,358 (“the ‘358 patent”) entitled, *Mechanism for Implementing Multiple Logical Routers Within A Single Physical Router*, was filed on July 9, 2002, and claims priority to July 9, 2001. The ‘358 patent is subject to a 35 U.S.C. § 154(b) term extension of 1,136 days. Sable Networks, Inc. is the owner by assignment of the ‘358 patent. Sable IP is the exclusive licensee of the ‘358 patent. A true and correct copy of the ‘358 patent is attached hereto as Exhibit C.

48. The ‘358 patent claims specific methods and systems for implementing multiple logical routers within a single physical router.

49. The ‘358 patent discloses systems and methods that combine the benefits of multi-routers and virtual routers. The logical routers are included within the same physical router; however, internal links permit improved efficiency over virtual routers because the technologies claimed in the ‘358 patent can take advantage of the fact that the logical routers are not standalone routers but are embodied in the same physical router.

50. The ‘358 patent discloses technology for implementing multiple logical routers within a single physical router.

51. The ‘358 patent discloses a router with a first set of one or more components capable of being figured to implement a first logical router within the router.

52. The ‘358 patent discloses a router with a second set of one or more components capable of being configured to implement a second logical router within the router.

53. The ‘358 patent discloses a router with a forwarding routing table that comprises an identifier that indicates an internal link is internal rather than an external link.

54. The ‘358 patent discloses a router wherein the first and second sets of components comprise functionality for establishing the internal link between the first logical router and the second logical router and advertising the internal link to other routers external to the router such that the first and second logical routers appear to the other routers as interconnected standalone routers, wherein the internal link is a logical, non-physical entity.

55. The ‘358 patent has been cited by 42 United States and international patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have all cited the ‘358 patent as relevant prior art:

- Cisco Systems, Inc.
- Dell Technologies, Inc.
- Juniper Networks, Inc.
- Nicira, Inc.
- International Business Machines Corporation
- NantWorks, LLC
- Telefonaktiebolaget LM Ericsson
- Verizon Communications, Inc.

#### **U.S. PATENT No. 8,243,593**

56. U.S. Patent No. 8,243,593 entitled, *Mechanism for Identifying and Penalizing Misbehaving Flows in a Network*, was filed on December 22, 2004. The ‘593 patent is subject to

a 35 U.S.C. § 154(b) term extension of 1,098 days. Sable Networks, Inc. is the owner by assignment of the '593 patent. Sable IP is the exclusive licensee of the '593 patent. A true and correct copy of the '593 patent is attached hereto as Exhibit D.

57. The '593 patent discloses novel methods and systems for processing a flow of a series of information packets.

58. The inventions disclosed in the '593 patent teach technologies that permit the identification and control of less desirable network traffic.

59. Because the characteristics of data packets in undesirable network traffic can be disguised, the '593 patent improves the operation of computer networks by disclosing technologies that monitor the characteristics of flows of data packets rather than ancillary factors such as port numbers or signatures.

60. The '593 patent discloses tracking the behavioral statistics of a flow of data packets that can be used to determine whether the flow is undesirable.

61. The '593 patent further discloses taking actions to penalize the flow of undesirable network traffic.

62. The '593 patent discloses a method for processing a flow of a series of information packets that maintains a set of behavioral statistics for the flow, wherein the set of behavioral statistics is updated based on each information packet belonging to the flow, as each information packet is processed.

63. The '593 patent discloses a method for processing a flow of a series of information packets that determines, based at least partially upon the set of behavioral statistics, whether the flow is exhibiting undesirable behavior.

64. The '593 patent discloses that the determination as to whether the flow is exhibiting undesirable behavior is made regardless of the presence or absence of congestion.

65. The '593 patent discloses a method for processing a flow of data packets that enforces a penalty on the flow in response to a determination that the flow is exhibiting undesirable behavior.

66. The '593 patent has been cited by 17 patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '593 patent as relevant prior art.

- Cisco Systems, Inc.
- AT&T, Inc.
- International Business Machines Corporation
- Telecom Italia S.p.A.
- McAfee, LLC

**COUNT I**  
**INFRINGEMENT OF U.S. PATENT NO. 6,954,431**

67. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

68. SonicWall designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for managing data traffic comprising a plurality of micro-flows through a network.

69. SonicWall designs, makes, sells, offers to sell, imports, and/or uses SonicWall network security appliances running SonicOS 6.2 or later, including: SonicWall TZ Series Firewalls (including at least the following models: TZ105W, TZ205, TZ205W, TZ215, TZ270, TZ270W, TZ300, TZ300P, TZ300W, TZ350, TZ350W, TZ370, TZ370W, TZ400, TZ400W, TZ470, TZ470W, TZ500, TZ500W, TZ570, TZ570P, TZ570W, TZ600, TZ600P, TZ670, SOHO,

SOHO W, SOHO 250, and SOHO 250W); SonicWall NSa Series Firewalls (including at least the following models: NSa 220, NSa 220W, NSa 250M, NSa 250MW, NSa 2600, NSa 2650, NSa 2700, NSa 3650, NSa 4650, NSa 5650, NSa 6650, NSa 9250, NSa 9450, and NSa 9650); SonicWall NSsp Series Firewalls (including at least the following models: NSsp 12400, NSsp 12800, and NSsp 15700); SonicWall SuperMassive Series Firewalls (including at least the following models: 9200, 9400, 9600, and 9800); and SonicWall E-Class Series Network Security Appliances (including at least the following models: E5599, E6500, and E8500) (collectively, the “SonicWall ‘431 Products(s)”).

70. One or more SonicWall subsidiaries and/or affiliates use the SonicWall ‘431 Products in regular business operations.

71. One or more of the SonicWall ‘431 Products include technology for managing data traffic comprising a plurality of micro-flows through a network.

72. One or more of the SonicWall ‘431 Products determine the capacity of a buffer containing a micro-flow based on a characteristic.

73. One or more of the SonicWall ‘431 Products assign an acceptable threshold value for the capacity of the buffer over a predetermined period of time.

74. One or more of the SonicWall ‘431 Products delegate a portion of available bandwidth in the network to the micro-flow.

75. The SonicWall ‘431 Products enable the setting of thresholds for a buffer that include the ability to set a threshold as a percentage of the buffer.

76. One or more of the SonicWall ‘431 Products use the buffer for damping jitter associated with the micro-flow.

77. The SonicWall ‘431 Products use buffers to limit jitter which is delay variance.

78. SonicWall has directly infringed and continues to directly infringe the '431 patent by, among other things, making, using, offering for sale, and/or selling technology for managing data traffic comprising a plurality of micro-flows through a network, including but not limited to the SonicWall '431 Products.

79. The SonicWall '431 Products are available to businesses and individuals throughout the United States.

80. The SonicWall '431 Products are provided to businesses and individuals located in the Western District of Texas.

81. By making, using, testing, offering for sale, and/or selling products and services for managing data traffic comprising a plurality of micro-flows through a network, including but not limited to the SonicWall '431 Products, SonicWall has injured Plaintiffs and is liable to Plaintiffs for directly infringing one or more claims of the '431 patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a).

82. SonicWall also indirectly infringes the '431 patent by actively inducing infringement under 35 USC § 271(b).

83. SonicWall has had knowledge of the '431 patent since at least service of this Complaint or shortly thereafter, and SonicWall knew of the '431 patent and knew of its infringement, including by way of this lawsuit.

84. SonicWall intended to induce patent infringement by third-party customers and users of the SonicWall '431 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. SonicWall specifically intended and was aware that the normal and customary use of the accused products would infringe the '431 patent. SonicWall performed the acts that

constitute induced infringement, and would induce actual infringement, with knowledge of the ‘431 patent and with the knowledge that the induced acts would constitute infringement. For example, SonicWall provides the SonicWall ‘431 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘431 patent, including at least claim 1, and SonicWall further provides documentation and training materials that cause customers and end users of the SonicWall ‘431 Products to utilize the products in a manner that directly infringe one or more claims of the ‘431 patent.<sup>19</sup> By providing instruction and training to customers and end-users on how to use the SonicWall ‘431 Products in a manner that directly infringes one or more claims of the ‘431 patent, including at least claim 1, SonicWall specifically intended to induce infringement of the ‘431 patent. SonicWall engaged in such inducement to promote the sales of the SonicWall ‘431 Products, e.g., through SonicWall user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘431 patent. Accordingly, SonicWall has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘431 patent, knowing that such use constitutes infringement of the ‘431 patent.

85. The ‘431 patent is well-known within the industry as demonstrated by multiple citations to the ‘431 patent in published patents and patent applications assigned to technology companies and academic institutions. SonicWall is utilizing the technology claimed in the ‘431

---

<sup>19</sup> See, e.g., *SonicWall SonicOS 6.5 System Setup Administration*, SONICWALL DOCUMENTATION (July 2020); *SonicWall SonicOS 6.2 Administration Guide*, SONICWALL DOCUMENTATION (November 2017); *SonicOS 6.5 Security Configuration Guide*, SONICWALL DOCUMENTATION (May 2020); *SonicOS 7 Rules and Policies Administration Guide*, SONICWALL DOCUMENTATION (January 2021); *SonicOS and SonicOSX 7 Users Administration Guide for the TZ and NSv Series*, SONICWALL DOCUMENTATION (August 2020); *SonicOS 6.5 NSsp 1 2000 / SM 9800 System Setup*, SONICWALL DOCUMENTATION (February 2019); *SonicOS Platform Data Sheet*, SONICWALL DOCUMENTATION (2019); *SonicOS 6.5 NSsp 12000 / SM 9800 Security Configuration Administration*, SONICWALL DOCUMENTATION (January 2019); *SonicWall SonicOS 6.5 NSv Policies Administration*, SONICWALL DOCUMENTATION (August 2019); and *SonicWall SonicOS API 6.5.4 Reference*, SONICWALL DOCUMENTATION (May 2019).

patent without paying a reasonable royalty. SonicWall is infringing the '431 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

86. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '431 patent.

87. As a result of SonicWall's infringement of the '431 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for SonicWall's infringement, but in no event less than a reasonable royalty for the use made of the invention by SonicWall together with interest and costs as fixed by the Court.

**COUNT II**  
**INFRINGEMENT OF U.S. PATENT No. 6,977,932**

88. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

89. SonicWall designs, makes, sells, offers to sell, imports, and/or uses SonicWall network security appliances running SonicOS 7.0 or later, including: SonicWall TZ Series Firewalls (including at least the following models: TZ270, TZ370, TZ470, TZ570, TZ670); SonicWall NSa Series Firewalls (including at least the following models: NSa2650, NSa2700, NSa3650, NSa4650, NSa5650), NSa 6650, NSa9250, NSa9450, NSa9650); and SonicWall NSsp Series Firewalls (including at least the following models: NSsp15700, NSsp12800, NSsp12400) (collectively, the "SonicWall '932 Products(s)").

90. One or more SonicWall subsidiaries and/or affiliates use the SonicWall '932 Products in regular business operations.

91. SonicWall has directly infringed and continues to directly infringe the '932 patent by, among other things, making, using, offering for sale, and/or selling technology that utilize flow state information to perform a method of network tunneling.

92. One or more of the SonicWall '932 Products utilize flow state information to perform a network tunneling method.

93. One or more of the SonicWall '932 Products create a flow block having flow state information for a received first data packet of a micro-flow.

94. One or more of the SonicWall '932 Products store a tunnel identifier for the micro-flow in the flow block, the tunnel identifier identifying a selected network tunnel to be used to transmit the data packet.

95. One or more of the SonicWall '932 Products index an aggregate flow block using the tunnel identifier.

96. One or more of the SonicWall '932 Products utilize an aggregate flow block with tunnel specific information for the selected network tunnel and that stores statistics for the selected network tunnel.

97. One or more of the SonicWall '932 Products transmit data packets using the selected network tunnel based on the tunnel specific information.

98. The SonicWall '932 Products are available to businesses and individuals throughout the United States.

99. The SonicWall '932 Products are provided to businesses and individuals located in the Western District of Texas.

100. By making, using, testing, offering for sale, and/or selling products utilizing flow state information to perform a method of network tunneling, including but not limited to the

SonicWall ‘932 Products, SonicWall has injured Plaintiffs and is liable to Plaintiffs for directly infringing one or more claims of the ‘932 patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a).

101. SonicWall also indirectly infringes the ‘932 patent by actively inducing infringement under 35 USC § 271(b).

102. SonicWall has had knowledge of the ‘932 patent since at least service of this Complaint or shortly thereafter, and SonicWall knew of the ‘932 patent and knew of its infringement, including by way of this lawsuit.

103. SonicWall intended to induce patent infringement by third-party customers and users of the SonicWall ‘932 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. SonicWall specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘932 patent. SonicWall performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘932 patent and with the knowledge that the induced acts would constitute infringement. For example, SonicWall provides the SonicWall ‘932 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘932 patent, including at least claim 1, and SonicWall further provides documentation and training materials that cause customers and end users of the SonicWall ‘932 Products to utilize the products in a manner that directly infringe one or more claims of the ‘932 patent.<sup>20</sup> By providing instruction and training to customers and end-

---

<sup>20</sup> See, e.g. *SonicOS and SonicOSX 7 Tools & Monitors Administration Guide*, SONICWALL DOCUMENTATION (August 2020); *SonicOSX 7 Rules and Policies Administration Guide*, SONICWALL DOCUMENTATION (August 2020); *Configure WAN Group VPN On A SonicWall Firewall*, SonicWall YouTube Channel (August 24, 2018), available at: <https://www.youtube.com/watch?sonicv=de2bnAlqz60>; *SonicWall SonicOS 6.5 Connectivity Administration*, SONICWALL DOCUMENTATION (July 2020); *SonicWall SonicOS 6.2.5 / 6.2.7 /*

users on how to use the SonicWall ‘932 Products in a manner that directly infringes one or more claims of the ‘932 patent, including at least claim 1, SonicWall specifically intended to induce infringement of the ‘932 patent. SonicWall engaged in such inducement to promote the sales of the SonicWall ‘932 Products, e.g., through SonicWall user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘932 patent. Accordingly, SonicWall has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘932 patent, knowing that such use constitutes infringement of the ‘932 patent.

104. The ‘932 patent is well-known within the industry as demonstrated by multiple citations to the ‘932 patent in published patents and patent applications assigned to technology companies and academic institutions. SonicWall is utilizing the technology claimed in the ‘932 patent without paying a reasonable royalty. SonicWall is infringing the ‘932 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

105. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘932 patent.

106. As a result of SonicWall’s infringement of the ‘932 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for SonicWall’s

---

*6.2.9 Log Events Reference Guide*, SONICWALL DOCUMENTATION (July 2017); *SonicWall SonicOS 6.5.1 Log Events Reference Guide*, SONICWALL DOCUMENTATION (June 2018); *SonicOS and SonicOSX 7 IPSec VPN Administration Guide*, SONICWALL DOCUMENTATION (August 2020); *SonicWall Network Security Appliance (NSa) Series Datasheet*, SONICWALL DOCUMENTATION (2020); *SonicWall NSa2700 Datasheet*, SONICWALL DOCUMENTATION (2020); and *SonicWall TZ Series (Gen 7) Integrated SD-Branch Platform For Next-Gen SMBs & Branches Datasheet*, SONICWALL DOCUMENTATION (2020).

infringement, but in no event less than a reasonable royalty for the use made of the invention by SonicWall together with interest and costs as fixed by the Court.

**COUNT III**  
**INFRINGEMENT OF U.S. PATENT NO. 7,630,358**

107. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

108. SonicWall designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for implementing multiple logical routers within a single physical router.

109. SonicWall designs, makes, sells, offers to sell, imports, and/or uses SonicWall Network Security NSv Series devices (including at least the following models: NSv1600, NSv870, NSv800, NSv470, NSv400, NSv300, NSv270, NSv200, NSv10, NSv25, NSv50, and NSv100) (the “SonicWall ‘358 Product(s)”).

110. One or more SonicWall subsidiaries and/or affiliates use the SonicWall ‘358 Products in regular business operations.

111. One or more of the SonicWall ‘358 Products include technology for implementing multiple logical routers within a single physical router.

112. One or more of the SonicWall ‘358 Products include a router with a first set of one or more components capable of being figured to implement a first logical router within the router.

113. One or more of the SonicWall ‘358 Products include a router with a second set of one or more components capable of being configured to implement a second logical router within the router.

114. One or more of the SonicWall ‘358 Products include a router with a forwarding routing table that comprises an identifier that indicates an internal link is internal rather than an external link.

115. One or more of the SonicWall '358 Products include a router wherein the first and second sets of components comprise functionality for establishing the internal link between the first logical router and the second logical router and advertising the internal link to other routers external to the router such that the first and second logical routers appear to the other routers as interconnected standalone routers, wherein the internal link is a logical, non-physical entity.

116. The SonicWall '358 Products are available to businesses and individuals throughout the United States.

117. The SonicWall '358 Products are provided to businesses and individuals located in the Western District of Texas.

118. SonicWall has directly infringed and continues to directly infringe the '358 patent by, among other things, making, using, offering for sale, and/or selling routers implementing multiple logical routers within a single physical router, including but not limited to the SonicWall '358 Products.

119. By making, using, testing, offering for sale, and/or selling routers implementing multiple logical routers within a single physical router, including but not limited to the SonicWall '358 Products, SonicWall has injured Plaintiffs and is liable for directly infringing one or more claims of the '358 patent, including at least claim 1, pursuant to 35 U.S.C. § 271(a).

120. SonicWall also indirectly infringes the '358 patent by actively inducing infringement under 35 USC § 271(b).

121. SonicWall has had knowledge of the '358 patent since at least service of this Complaint or shortly thereafter, and SonicWall knew of the '358 patent and knew of its infringement, including by way of this lawsuit.

122. SonicWall intended to induce patent infringement by third-party customers and users of the SonicWall ‘358 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. SonicWall specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘358 patent. SonicWall performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘358 patent and with the knowledge that the induced acts would constitute infringement. For example, SonicWall provides the SonicWall ‘358 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘358 patent, including at least claim 1, and SonicWall further provides documentation and training materials that cause customers and end users of the SonicWall ‘358 Products to utilize the products in a manner that directly infringe one or more claims of the ‘358 patent.<sup>21</sup> By providing instruction and training to customers and end-users on how to use the SonicWall ‘358 Products in a manner that directly infringes one or more claims of the ‘358 patent, including at least claim 1, SonicWall specifically intended to induce infringement of the ‘358 patent. SonicWall engaged in such inducement to promote the sales of the SonicWall ‘358 Products, e.g., through SonicWall user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘358 patent. Accordingly, SonicWall has induced and continues to induce users of the accused

---

<sup>21</sup> See, e.g., *SonicWall Network Security Virtual (Nsv) Firewall Series Next-Gen Security For Public, Private Or Hybrid Cloud Environments*, SONICWALL DOCUMENTATION (2021); *SonicWall SonicOS 6.5 NSv System Setup Administration*, SONICWALL DOCUMENTATION (2020); *SonicWall NSv Series on AWS Getting Started Guide (BYOL / PAYG)*, SONICWALL DOCUMENTATION (December 2020); *SonicWall SonicOS 6.5 NSv Policies Administration*, SONICWALL DOCUMENTATION (2020); *SonicWall SonicOS 6.5 NSv Investigate Administration*, SONICWALL DOCUMENTATION (May 2019); *SonicWall SonicOS 6.5 NSv Monitor Administration*, SONICWALL DOCUMENTATION (May 2019); and *SonicOS 6.5 for NSv Series Security Configuration Administration Guide*, SONICWALL DOCUMENTATION (October 2018).

products to use the accused products in their ordinary and customary way to infringe the '358 patent, knowing that such use constitutes infringement of the '358 patent.

123. The '358 patent is well-known within the industry as demonstrated by multiple citations to the '358 patent in published patents and patent applications assigned to technology companies and academic institutions. SonicWall is utilizing the technology claimed in the '358 patent without paying a reasonable royalty. SonicWall is infringing the '358 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

124. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '358 patent.

125. As a result of SonicWall's infringement of the '358 patent, Plaintiffs have suffered monetary damages, and seeks recovery in an amount adequate to compensate for SonicWall's infringement, but in no event less than a reasonable royalty for the use made of the invention by SonicWall together with interest and costs as fixed by the Court.

**COUNT IV**  
**INFRINGEMENT OF U.S. PATENT NO. 8,243,593**

126. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

127. SonicWall designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for processing a flow of a series of information packets.

128. SonicWall designs, makes, sells, offers to sell, imports, and/or uses SonicWall network security appliances running SonicOS 6.2 or later, including: SonicWall TZ Series Firewalls (including at least the following models: SOHO W, SOHO 250, SOHO 250W, TZ300, TZ300P, TZ300W, TZ350, TZ350W, TZ400, TZ400W, TZ500, TZ500W, TZ600, TZ600P);

SonicWall SuperMassive 9000 Series Firewalls (including at least the following models: SM9200, SM9400, SM9600); and SonicWall NSa Series Firewalls (including at least the following models: NSa 2600, NSa 3600, NSa 4600, NSa 5600, NSa 6600, NSa2 650, NSa 3650, NSa 4650, NSa 5650, NSa 6650, NSa 9250, NSa 9450, NSa 9650) (collectively, the “SonicWall ‘593 Product(s)”).

129. One or more SonicWall subsidiaries and/or affiliates use the SonicWall ‘593 Products in regular business operations.

130. One or more of the SonicWall ‘593 Products include technology for processing a flow of a series of information packets. Specifically, the SonicWall ‘593 Products maintain a set of behavioral statistics based on each and every information packet belonging to a flow.

131. The SonicWall ‘593 Products are available to businesses and individuals throughout the United States.

132. The SonicWall ‘593 Products are provided to businesses and individuals located in the Western District of Texas.

133. SonicWall has directly infringed and continues to directly infringe the ‘593 patent by, among other things, making, using, offering for sale, and/or selling products and services for processing a flow of a series of information packets.

134. The SonicWall ‘593 Products maintain a set of behavioral statistics for the flow, wherein the set of behavioral statistics is updated based on each information packet belonging to the flow, as each information packet is processed.

135. The SonicWall ‘593 Products enable the generation of behavioral statistics based on each packet that is processed.

136. The SonicWall ‘593 Products determine, based at least partially upon the set of behavioral statistics, whether the flow is exhibiting undesirable behavior.

137. The SonicWall ‘593 Products determine whether the flow is exhibiting undesirable behavior regardless of the presence or absence of congestion.

138. The SonicWall ‘593 Products enforce a penalty on the flow in response to a determination that the flow is exhibiting undesirable behavior.

139. By making, using, testing, offering for sale, and/or selling products and services for processing a flow of a series of information packets, including but not limited to the SonicWall ‘593 Products, SonicWall has injured Plaintiffs and is liable for directly infringing one or more claims of the ‘593 patent, including at least claim 4, pursuant to 35 U.S.C. § 271(a).

140. SonicWall also indirectly infringes the ‘593 patent by actively inducing infringement under 35 USC § 271(b).

141. SonicWall has had knowledge of the ‘593 patent since at least service of this Complaint or shortly thereafter, and SonicWall knew of the ‘593 patent and knew of its infringement, including by way of this lawsuit.

142. SonicWall intended to induce patent infringement by third-party customers and users of the SonicWall ‘593 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. SonicWall specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘593 patent. SonicWall performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘593 patent and with the knowledge that the induced acts would constitute infringement. For example, SonicWall provides the SonicWall ‘593 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘593 patent, including at least claim 4, and SonicWall further provides documentation and training materials that cause customers and end

users of the SonicWall ‘593 Products to utilize the products in a manner that directly infringe one or more claims of the ‘593 patent.<sup>22</sup> By providing instruction and training to customers and end-users on how to use the SonicWall ‘593 Products in a manner that directly infringes one or more claims of the ‘593 patent, including at least claim 4, SonicWall specifically intended to induce infringement of the ‘593 patent. SonicWall engaged in such inducement to promote the sales of the SonicWall ‘593 Products, e.g., through SonicWall user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘593 patent. Accordingly, SonicWall has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘593 patent, knowing that such use constitutes infringement of the ‘593 patent.

143. The ‘593 patent is well-known within the industry as demonstrated by multiple citations to the ‘593 patent in published patents and patent applications assigned to technology companies and academic institutions. SonicWall is utilizing the technology claimed in the ‘593 patent without paying a reasonable royalty. SonicWall is infringing the ‘593 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

---

<sup>22</sup> See, e.g., *SonicWall SonicOS 6.2 Administration Guide*, SONICWALL DOCUMENTATION at 113 (2017); M.G. Sriram Iyer, *How to Configure Stateful Active-Standby High Availability in Gen6 UTM Appliances*, SONICWALL DELL EMC SUPPORT YOUTUBE CHANNEL (September 30, 2014), available at: <https://www.youtube.com/watch?v=OillXUxSqa0>; *SonicWall Network Security Appliance (NSa) Series Datasheet*, SONICWALL DATASHEET (2018); *SonicOS Platform Datasheet*, SONICWALL DOCUMENTATION (2018); *SonicWall SonicOS 6.5 System Setup Administration*, SONICWALL DOCUMENTATION (July 2020); *SonicWall SonicOS 6.2 Administration Guide*, SONICWALL DOCUMENTATION (November 2017); *SonicOS 6.5 Security Configuration Guide*, SONICWALL DOCUMENTATION (May 2020); *SonicOS 7 Rules and Policies Administration Guide*, SONICWALL DOCUMENTATION (January 2021); *SonicOS and SonicOSX 7 Users Administration Guide for the TZ and NSv Series*, SONICWALL DOCUMENTATION (August 2020); and *SonicOS 6.5 NSsp 1 2000 / SM 9800 System Setup*, SONICWALL DOCUMENTATION (February 2019).

144. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘593 patent.

145. As a result of SonicWall’s infringement of the ‘593 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for SonicWall’s infringement, but in no event less than a reasonable royalty for the use made of the invention by SonicWall together with interest and costs as fixed by the Court.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs Sable IP, LLC and Sable Networks, Inc. respectfully request that this Court enter:

- A. A judgment in favor of Plaintiffs that SonicWall has infringed, either literally and/or under the doctrine of equivalents, the ‘431, ‘932, ‘358, and ‘593 patents;
- B. An award of damages resulting from SonicWall’s acts of infringement in accordance with 35 U.S.C. § 284;
- C. A judgment and order finding that SonicWall’s infringement was willful, wanton, malicious, bad-faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate within the meaning of 35 U.S.C. § 284 and awarding to Plaintiffs enhanced damages.
- D. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiffs their reasonable attorneys’ fees against SonicWall.
- E. Any and all other relief to which Plaintiffs may show themselves to be entitled.

**JURY TRIAL DEMANDED**

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiffs Sable IP, LLC and Sable Networks, Inc. request a trial by jury of any issues so triable by right.

Dated: March 1, 2021

Respectfully submitted,

/s/ Daniel P. Hipskind

Dorian S. Berger (CA SB No. 264424)  
Daniel P. Hipskind (CA SB No. 266763)  
BERGER & HIPSKIND LLP  
9538 Brighton Way, Ste. 320  
Beverly Hills, CA 90210  
Telephone: 323-886-3430  
Facsimile: 323-978-5508  
E-mail: dsb@bergerhipskind.com  
E-mail: dph@bergerhipskind.com

Elizabeth L. DeRieux  
State Bar No. 05770585  
Capshaw DeRieux, LLP  
114 E. Commerce Ave.  
Gladewater, TX 75647  
Telephone: 903-845-5770  
E-mail: ederieux@capshawlaw.com

*Attorneys for Sable Networks, Inc. and  
Sable IP, LLC*